

What's New in VMware vCloud Director 8.10

Feature Overview

TECHNICAL WHITE PAPER

Table of Contents

- Introduction 3
- Architecture Updates 3
 - Single IP Address for UI and Console Proxy 3
 - Object Extensibility for Customized VM Placement 3
 - Unattended Install 4
 - VMware NSX 6.1.x and 6.2.x Support 4
- Feature Updates 4
 - User Interface 4
 - Distributed Resource Scheduler Affinity and Anti-Affinity for VMs 6
 - VDC Permissions API 10
 - Advanced VM Settings 12
 - VMware vRealize Orchestrator Plug-in 14
 - Additional Changes 14
- Summary 14

Introduction

The VMware vCloud Director® software solution enables service providers to orchestrate the provisioning of virtual data centers (VDCs) that are software-defined, modular, and ready for consumption in a matter of minutes.

Version 8.10 of vCloud Director software includes an enhanced architecture and new features that provide an even better and more robust platform for delivering infrastructure-as-a-service (IaaS) solutions:

- Stronger performance elements to handle latency-sensitive workloads
- Support for VMware NSX® 6.1.x and 6.2.x for networking, along with VMware vSphere® 6.0 up to virtual hardware version 11
- Support for Windows 10 as a guest operating system (Refer to the VMware product interoperability matrix to see the most recent support: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.)
- Additional user interface (UI) capabilities for features that were previously available via API only

Architecture Updates

The vCloud Director software solution has an updated architecture that incorporates security and provides service providers with the flexibility to place virtual machines (VMs) in vSphere clusters.

Single IP Address for UI and Console Proxy

Previously, vCloud Director software required two IP addresses to support two SSL endpoints: One was used as the overall UI and API endpoint for Web portal and API calls, and the other was used for listening to console proxy requests that allowed users to log in to the VMs via their consoles. This vCloud Director release removes the need to have two sets of IP addresses for an install and can now use a single IP address with two different ports as SSL endpoints instead.

During vCloud Director installation, the install script will ask for two different ports: one to listen for UI and API calls, and one to listen for console proxy and vCloud Director remote console requests.

If upgrading a vCloud Director instance from an earlier version of vCloud Director software, version 8.10 will continue to support the use of two IP addresses for endpoints.

Object Extensibility for Customized VM Placement

Organization administrators managing multiple VDCs might have different requirements for placing VMs, depending on the type of workload or user that's making the request. vCloud Director 8.10 introduces the ability to customize some VM placement and deployment decisions. This provides greater flexibility and overall environment control.

The vCloud Director software solution has predefined and built-in algorithms to select a specific resource pool and determine where a new VM should be placed when a request is made. Certain objects in the vCloud Director workflow have been extended so that organization administrators can now amend the placement and deployment algorithms based on their organization's environment-specific needs.

The following vCloud Director objects can integrate with externally registered extensions that have the algorithmic logic that implements or defines the necessary custom rules:

- VM placement
- VM deployment
- VDC template instantiation

Each of these extensions can have multiple rules with assigned ranks for conflict resolution. These extensions are registered via the vCloud Director Extensions API, and they communicate via an Advanced Message Queuing Protocol (AMQP) messaging bus.

Unattended Install

It is now possible to install vCloud Director software using the configuration utility. The utility allows a user to supply all the necessary configuration options in a single command and, when used in conjunction with an “unattended” flag, the install will be silent and noninteractive:

```
Configuration-tool -ip 10.150.153.121 -dbhost 10.150.152.246 -dbport 1433  
-dbname vcloud -dbuser vcloud -dbpassword akimbi -dbtype sqlserver -dbinstance  
MSSQLSERVER -k /certs -w passwd -cons 172.17.42.1 -unattended
```

VMware NSX 6.1.x and 6.2.x Support

vCloud Director 8.10 is now even more tightly integrated with VMware NSX network virtualization, relying solely on the VMware NSX Manager™ platform for providing networking functions to VDCs.

vCloud Director 8.10 now deploys VMware NSX Edge™ gateways by default whenever a new organization edge is created. In vCloud Director 8.0 and earlier versions, NSX network virtualization operated in a backward-compatible mode, and VMware vCloud Networking and Security Edge™ gateways were deployed by default. NSX Edge gateways have tremendous performance and stability advantages, and they support dynamic routing with both the Open Shortest Path First (OSPF) routing protocol and Border Gateway Protocol (BGP). NSX Edge gateways also support Layer 2 VPNs and have high availability built in.

Feature Updates

The vCloud Director software solution has a number of updated features that give service providers greater flexibility for customizing their VDCs, both from APIs and the user interface.

User Interface

vCloud Director 8.10 adds more functionality to the user interface. Certain tasks and actions that were previously only accessible via the vCloud Director REST API can now be performed from the vCloud Director user interface or Web portal.

VDC Limits

Organization VDCs often have lease restrictions, such as quotas on the number of VMs that users can have and limits on how long virtual appliances (vApps) are allowed to run before expiring. vCloud Director 8.10 adds the ability to limit the number of VDCs that can be created in an organization. This setting can be accessed by right-clicking Organization > Properties > Policies.



Figure 1. Organization VDC Limits

Tenant Throttling

Tenant throttling can be used to limit the number of operations that tenants can perform, so that requests from a “busy” tenant do not stop or slow requests from more “sedentary” tenants. The feature was introduced in vCloud Director 8.0, but it was only accessible via the REST API. Now this setting can be accessed by right-clicking Organization > Properties > Policies.

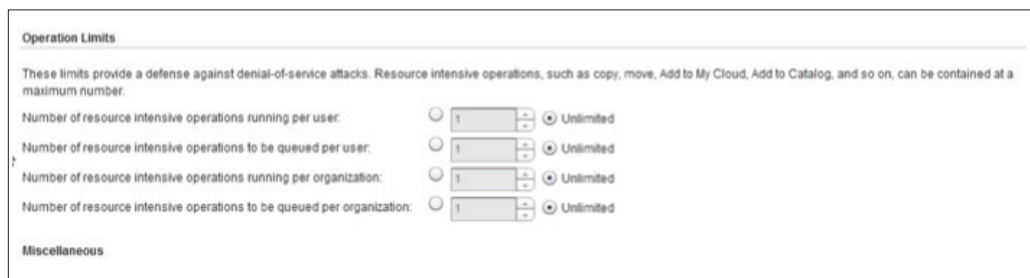


Figure 2. Tenant Throttling Limits

Organization VDC Templates

VDC templates provide a standard specification for new VDCs that approved users within tenant organizations deploy. They allow system administrators to predefine the characteristics of new VDCs. Organization users can then self-provision VDCs without further system administrator assistance.

System administrators can specify template characteristics such as the provider VDC that the organization VDC template should be bound to upon creation and the organization networks that are allowed to be attached.

Access the template creation from the Manage & Monitor tab > Organization VDC Templates.

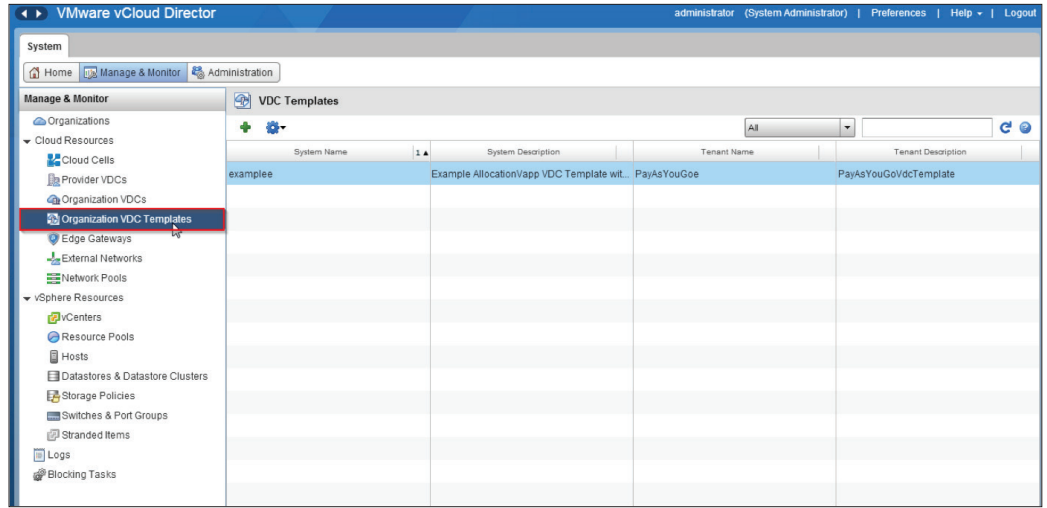


Figure 3. Organization VDC Templates UI

Distributed Resource Scheduler Affinity and Anti-Affinity for VMs

The vCloud Director product leverages the VMware vSphere Distributed Resource Scheduler™ (DRS) utility at the compute cluster level to distribute the VMs deployed in an organization's VDCs. Normally, the DRS setting on the vSphere cluster ensures that workloads are evenly spread across the VMware ESXi™ hosts. However, certain performance-sensitive applications might require multiple VMs to remain on the same ESXi host while being deployed. In this case, the VMs need to have an affinity rule set between them. The new affinity rule feature introduced in vCloud Director 8.10 can be used to specify which VMs need to be together, and the vSphere DRS utility will then place them on the same ESXi host.

Other workloads may require individual VMs to be distributed across the ESXi hosts in a cluster, for example, in the case of host failover and application continuation conditions. This would require setting anti-affinity rules between the VMs of the workload. The affinity and anti-affinity settings can be accessed via Organization VDC Properties > Affinity Rules.

To create a new affinity or anti-affinity rule, click the plus sign (+) and identify which VMs should be part of the rules.

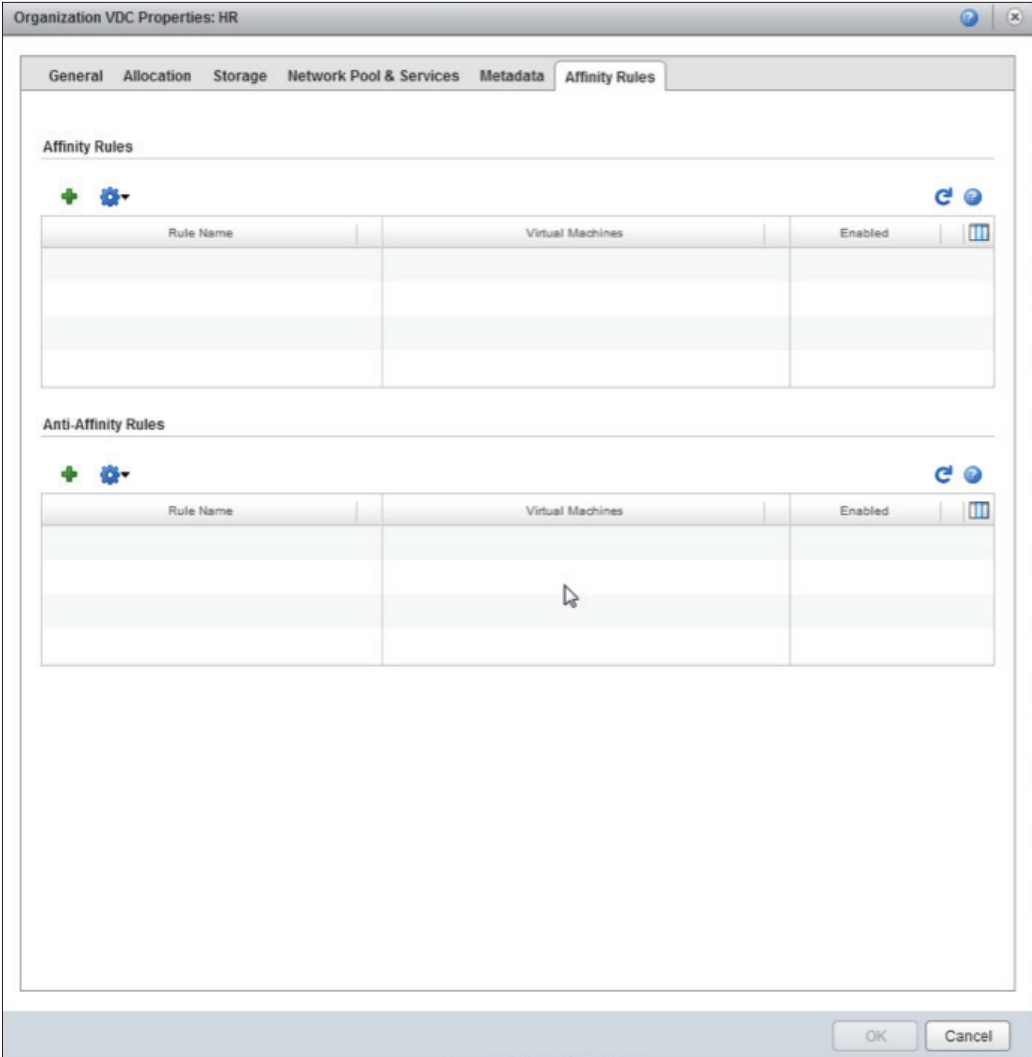


Figure 4. Affinity Rules for the Organization VDC

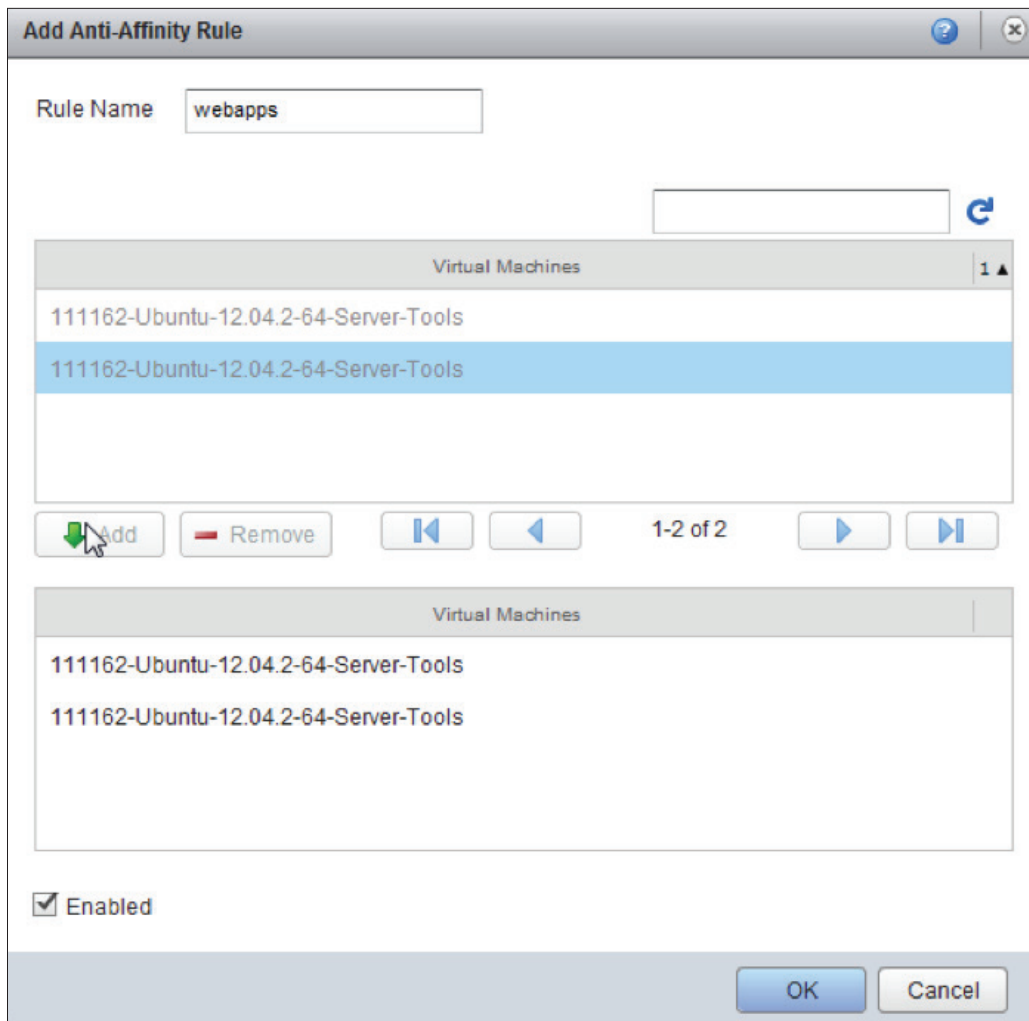


Figure 5. Adding Affinity Rules on VMs

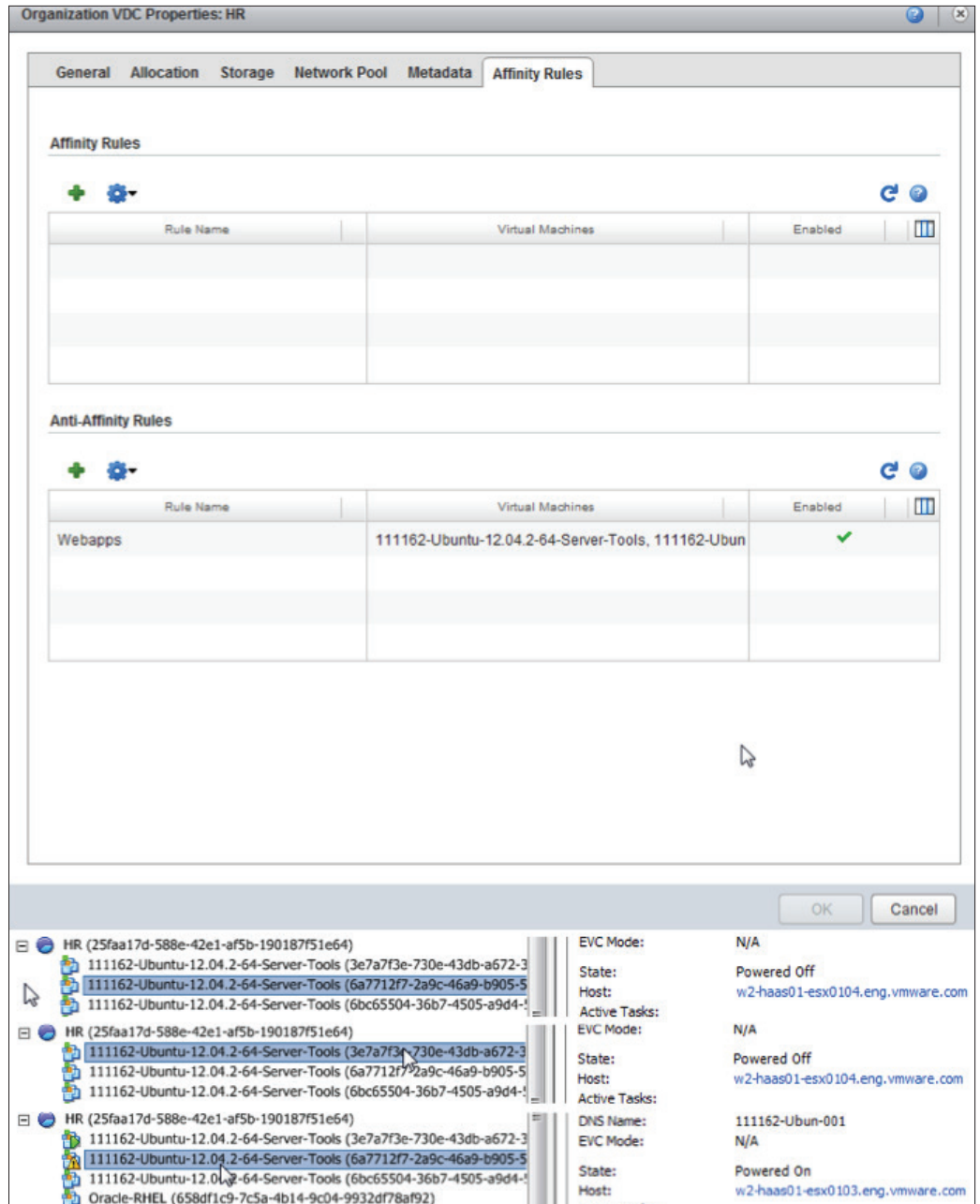


Figure 6. After Affinity Rule Is Added, vSphere DRS Redistributes VM

Once the rule is set, vCloud Director software will pass the settings along to the corresponding vSphere cluster backing the organization VDC, and a corresponding DRS rule will be created within the vSphere environment. If the VMs were on the same ESXi host and an anti-affinity policy is set, vSphere DRS will use the VMware vSphere vMotion® feature to move the VMs to the next ESXi host that is part of the cluster. (Note: The affinity and anti-affinity settings are applied between VMs, not between a VM and ESXi host.)

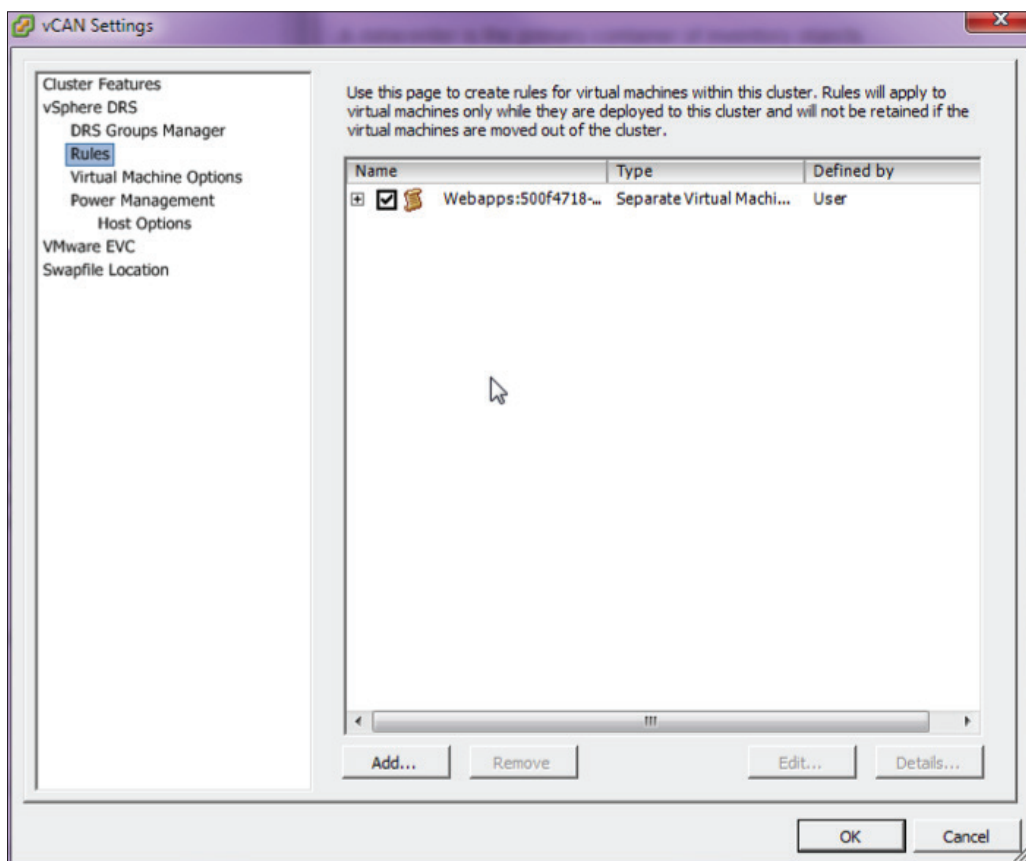


Figure 7. Affinity Rules Set on vSphere DRS Cluster by VMware vCloud Director Software

VDC Permissions API

When users are added at an organization level, their access to the VDCs in the organization is either all in or all out: If they can see one VDC, they can see all the VDCs defined for that particular organization. However, the new VDC Permissions API feature allows user access to be restricted to a specific VDC within the organization.

A VDC can also be set to be shared, which means that even if an access control list exists, it will be ignored for that VDC. The access rule can be created using the controlAccess API on the organization VDC.

ControlAccess API

The ControlAccess API can be used to show the access status of a VDC. A VDC with <IsSharedToEveryone> set to true will be visible to all users; if set to false, the VDC will be visible to users who are defined as part of the access control list:

GET /api/vdc/{id}/controlAccess

```
<?xml version="1.0" encoding="UTF-8"?>
<ControlAccessParams
  xmlns="http://www.vmware.com/vcloud/v1.5"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.vmware.com/vcloud/v1.5 http://10.115.73.160/api/
v1.5/schema/master.xsd">
  <IsSharedToEveryone>true</IsSharedToEveryone>
  <EveryoneAccessLevel>ReadOnly</EveryoneAccessLevel>
</ControlAccessParams>
```

ReadOnly Setting

In this version of vCloud Director software, an access level set to ReadOnly means that the users listed in the access control list can see the new VDC being created but cannot use it to deploy any workloads. The system administrator can deploy new workloads and work on a proof of concept in the newly created VDC:

GET /api/vdc/(vDC-ID)/action/controlAccess

Content-Type: application/vnd.vmware.vcloud.controlAccess+xml

```
<?xml version="1.0" encoding="UTF-8"?>
<ControlAccessParams xmlns="http://www.vmware.com/vcloud/v1.5">
  <IsSharedToEveryone>false</IsSharedToEveryone>
  <AccessSettings>
    <AccessSetting>
      <ExternalSubject>
        <SubjectId>user1</SubjectId>
        <IsUser>true</IsUser>
        <IdpType>SAML</IdpType>
      </ExternalSubject>
      <AccessLevel>ReadOnly</AccessLevel>
    </AccessSetting>
  </AccessSettings>
</ControlAccessParams>
```

Response to Control Access Request

```
<?xml version="1.0" encoding="UTF-8"?>
<ControlAccessParams
  xmlns="http://www.vmware.com/vcloud/v1.5"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.vmware.com/vcloud/v1.5 http://10.115.73.160/api/
v1.5/schema/master.xsd">
  <IsSharedToEveryone>>false</IsSharedToEveryone>
  <AccessSettings>
    <AccessSetting>
      <Subject href="https://10.115.73.160/api/admin/user/07362841-
99d4-43bd-bd19-39f7495bbe8e" name="user1" type="application/vnd.vmware.admin.
user+xml"/>
      <AccessLevel>ReadOnly</AccessLevel>
    </AccessSetting>
    <AccessSetting>
      <Subject href="https://10.115.73.160/api/admin/user/7a4516b9-
c66d-4b9d-b328-3d6ad7e70f92" name="user2" type="application/vnd.vmware.admin.
user+xml"/>
      <AccessLevel>ReadOnly</AccessLevel>
    </AccessSetting>
  </AccessSettings>
</ControlAccessParams>
```

Advanced VM Settings

For workloads running latency-sensitive applications, vCloud Director 8.10 now recognizes advanced vSphere VM properties that are defined in the ExtraConfig section of the Open Virtualization Format (OVF) of a vApp template. When a VM with these properties is placed on the underlying vSphere resource pool, the vCloud Director software solution ensures that the properties are passed on to the vSphere platform and that VMware vCenter™ software can manage the vApp accordingly.

These advanced settings are already part of the vSphere platform and are used when latency-sensitive workloads need specific configurations to prevent the degradation of application performance. They ensure that the hypervisor will take special care when scheduling compute and network resources for the VM.

vCloud Director software can be configured to allow users with specific roles to set the ExtraConfig section properties. Such users can set any key-value pair defined by the OVF standard for the ExtraConfig section. In addition, the following are the specific ExtraConfig key-value pairs that can be assigned to a role:

- `sched.cpu.latencySensitivity` – When set to High, this will ensure the ESXi hypervisor will take extra care with overall resources scheduling for this VM.
- `ethernetn.coalescingScheme` – This property will disable network interrupt coalescing. Instead of the VM sending network interrupts periodically, this setting will help batch the interrupts, offloading constant hypervisor scheduling of CPU cycles for the interrupts.
- `numa.nodeAffinity` – This setting can help set the non-uniform memory access (NUMA) node affinity for a specific VM to a specific socket (n) on the CPU.

Users who want access to these features must have the appropriate rights to deploy a vApp with the ExtraConfig section settings.

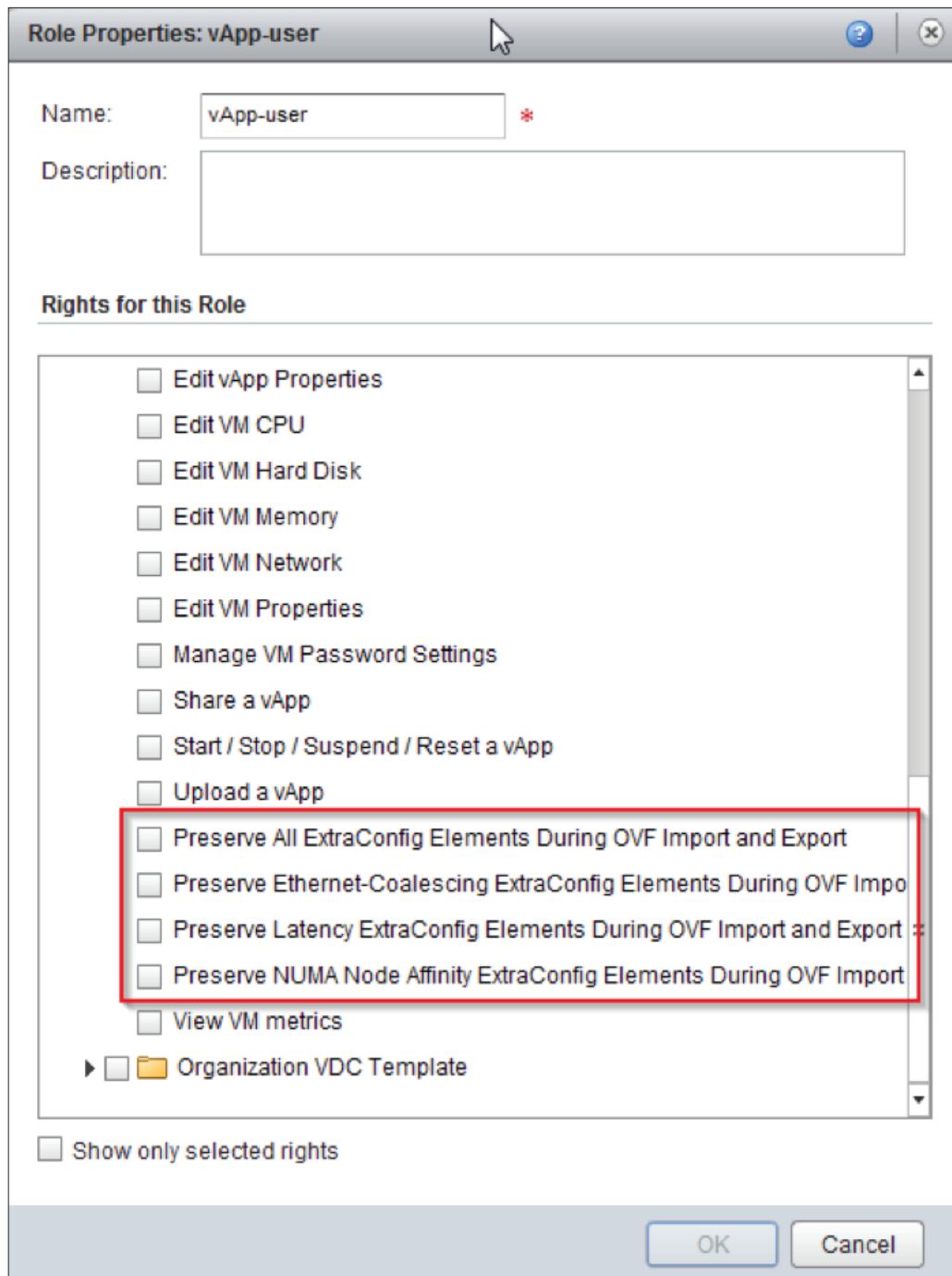


Figure 8. User Role Assignment for Advanced VM Settings

VMware vRealize Orchestrator Plug-in

The VMware vRealize® Orchestrator™ plug-in for the vCloud Director software solution has been updated to include the following workflows involving the vSphere DRS affinity/anti-affinity features:

- Retrieve a list of VM affinity rules.
- Add a VM affinity rule.
- Retrieve a VM affinity rule.
- Update a VM affinity rule.
- Delete a VM affinity rule.

Additional Changes

vCloud Director 8.10 improves other existing features:

- While deploying vApps from a catalog with guest customization enabled, the guest customization status can be queried with the help of an API call.
- Running VMs can now be copied or moved from the vSphere environment into an organization VDC. Previously, in vCloud Director 8.0 and earlier, users could only import VMs that were powered off.

Summary

The VMware vCloud Director 8.10 release focuses on improving application and workload performance. It provides access to some of the native vSphere features widely used by performance-sensitive applications on the abstraction layers created in organizations and organization VDCs.

More Information

For more information about the VMware vCloud Director software solution, visit the product pages at <http://www.vmware.com/products/vcloud-director/overview.html>.

Access the documentation for vCloud Director software at https://www.vmware.com/support/pubs/vcd_sp_pubs.html.

Access reference design and architecture documentation at <https://www.vmware.com/cloud-computing/cloud-architecture/vcat-sp.html>.

To purchase the vCloud Director software solution or to find out how you can join the VMware vCloud Air™ Network service provider program, visit <https://www.vmware.com/partners/service-provider/>.

About the Author

Boskey Savla is a senior technical marketing manager for the vCloud Air Network group at VMware. She works on developing resources for vCloud Air Network partners with various VMware product stacks, focusing on the VMware vCloud Director software solution. She has more than 12 years of experience in systems and solution engineering. She has worked with various VMware partners in certifying and architecting Software-Defined Data Centers and hybrid cloud solutions.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VM-3184-Whats-New-WMW-vCD-8-10-White-Paper-D1.2